Robert C. Schubert (S.B.N. 62684)
Dustin L. Schubert (S.B.N. 254876)
Amber L. Schubert (S.B.N. 278696)
SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, California 94123
Telephone: (415) 788-4220
Fax: (415) 788-0161
rschubert@sjk.law
dschubert@sjk.law
aschubert@sjk.law

Counsel for Plaintiffs Joseph De Rivera, Irwin Ojeda, and d'Amileau Baulk and the Putative Classes

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

JOSEPH DE RIVERA, IRWIN OJEDA, and d'AMILEAU BAULK, Individually and on Behalf of a Class of All Others Similarly Situated, Plaintiffs, v. CITY OF HOPE NATIONAL MEDICAL CENTER d/b/a CITY OF HOPE, Defendant.	**Case No.** **CLASS ACTION COMPLAINT** **Jury Trial Demanded**

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

Upon personal knowledge as to their own acts, and based upon their investigation, the investigation of counsel, and information and belief as to all other matters, Plaintiffs Joseph De Rivera, Irwin Ojeda, and d'Amileau Baulk, on behalf of themselves and all others similarly situated, allege as follows:

SUMMARY OF THE ACTION

1. Plaintiffs bring this class action against City of Hope National Medical Center d/b/a City of Hope ("City of Hope") for its failure to adequately secure and safeguard their and at least 827,149 total individuals' personally identifying information ("PII") and protected health information ("PHI"), including names, email addresses, phone numbers, dates of birth, Social Security numbers, driver's licenses or other government identifications, financial details such as bank account numbers and credit card information, health insurance information, medical records and medical histories, including medical conditions, among other potentially sensitive, private, and confidential data.

2. City of Hope is National Cancer Institute-designated comprehensive cancer center with research and treatment facilities located in California, Arizona, Illinois, and Georgia. In 2022, City of Hope provided care to over 131,000 patients.[1] City of Hope purports to be "committed" to protecting the privacy of its patients[2] and its Notice of Privacy Practices recognize City of Hope's legal obligation "to maintain the privacy of your protected health information."[3]

---

[1] 2022 Annual Report, CITY OF HOPE, *available at* https://www.cityofhope.org/sites/www/files/2023-10/2022-Annual-Report.pdf.

[2] *See Notice of Data Security Incident*, CITY OF HOPE (Apr. 2, 2024), https://www.cityofhope.org/notice-of-data-security-incident (last visited Apr. 29, 2024).

[3] *Notice of Privacy Practices*, CITY OF HOPE, *available at* https://www.cityofhope.org/sites/www/files/2024-03/COH-Notice-of-Privacy-Practices-09-2023_English.pdf.

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

3. In the ordinary course of providing healthcare services to its patients and other persons and employing its staff, individuals provided City of Hope (or City of Hope otherwise received) PII and PHI from at least hundreds of thousands of persons. In turn, City of Hope comes into the possession of, and maintains extensive files containing, the PII and PHI of its patients, data subjects, employees, and other persons, and owes these individuals an affirmative duty to adequately protect and safeguard this private information against theft and misuse. Despite such duties created by statute, regulation, and common law, at all relevant times, City of Hope utilized deficient data security practices, thereby allowing hundreds of thousands of persons' sensitive and private data to fall into the hands of strangers.

4. Between September 19, 2023 and October 12, 2023, City of Hope lost control over this highly sensitive and confidential PII and PHI of Plaintiffs and the Class Members (defined herein) in a massive and preventable data breach apparently perpetrated by cybercriminals (the "Data Breach"). According to City of Hope, on October 13, 2023, it "became aware of suspicious activity on a subset of its systems."[4] City of Hope has not explained what, if anything, it did to cut off the bad actors' access to its systems, but claims to have "immediately instituted mitigation measures to minimize and contain any disruption to its operations."[5] Thereafter, City of Hope also launched an investigation with assistance from cybersecurity professionals, who determined that an unauthorized third party was able to obtain copies of "some" of City of Hope's files. Altogether, cybercriminals had unfettered access to Plaintiffs' and the Class's highly private information for over three weeks (twenty-three days in total).[6]

[4] *Notice of Data Security Incident*, CITY OF HOPE, *supra* note 2.

[5] *See id.*

[6] *Id.*

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

5. The Data Breach was directly and proximately caused by City of Hope's failure to implement and maintain reasonable and industry-standard data security practices necessary to protect its systems from a foreseeable and preventable cyberattack. Through this wrongful conduct, the sensitive PII and PHI of more than 820,000 individuals is now in the hands of cybercriminals, who target this sensitive data for its value to identity thieves. Plaintiffs and Class Members are now at a significantly increased and impending risk of fraud, identity theft, and similar forms of criminal mischief—risks which may last the rest of their lives. Consequently, Plaintiffs and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes. Moreover, Plaintiffs and Class Members have lost the inherent value of their private data.

6. By aggregating information obtained from the Data Breach with other sources or other methods, criminals can assemble a full dossier of private information on an individual to facilitate a wide variety of frauds, thefts, and scams. Criminals can and do use victims' names and other personal information to open new financial accounts, incur credit and bank charges on existing accounts, obtain government benefits and identifications, fabricate identities, and file fraudulent tax returns well before the person whose PII was stolen becomes aware of it. Any one of these instances of identity theft can have devastating consequences for the victim, causing years of often irreversible damage to their credit scores, financial stability, and personal security. Likewise, the exfiltration of protected health information puts Plaintiffs and the Class Members at a present and continuing risk of medical identity theft, which poses an even more critical threat to victims because such fraud could lead to loss of access to necessary healthcare through misuse of paid-for insurance benefits or by incurring substantial medical debt.

7. Despite the Data Breach being first detected on October 13, 2023, City of Hope only began notifying some impacted persons ***nearly two months later***, on December 14, 2023. However, the bulk of the Data Breach notices issued much later,

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

around April 2, 2024—***more than five months*** after City of Hope learned of the Data Breach. This significant delay exacerbated the damages and risks to Class Members, and violated various state data breach notification statutes and rules promulgated under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The Data Breach notice letters to victims also obscure the true nature of the City of Hope cyberattack and threat it posed—failing to adequately inform Plaintiffs and Class Members how many people were impacted, how the "unauthorized third party" accessed City of Hope's systems, copied its files, and the root cause of the Data Breach, what specific PII and PHI was stolen for each affected person, whether the exfiltrated information was encrypted or anonymized, why it took so long to notify victims, whether City of Hope or law enforcement have apprehended or even identified the hackers who accessed City of Hope's systems, or what specific remedial steps City of Hope has taken to safeguard PII and PHI within its systems and networks (or otherwise purge unnecessary information) and to prevent further cyberattacks going forward. Without these critical details, Plaintiffs and Class Members cannot meaningfully mitigate the resulting effects of the City of Hope Data Breach.

8. Plaintiffs De Rivera, Ojeda, and Baulk are all Data Breach victims and first received a notification of the Data Breach from City of Hope by letters dated April 2, 2024.

9. Plaintiffs, on behalf of themselves and all others similarly situated, herein allege claims for negligence, negligence *per se*, breach of implied contract, unjust enrichment or quasi-contract, invasion of privacy, violation of California's Confidentiality of Medical Information Act (CAL. CIV. CODE §§ 56, *et seq.*), violation of California's Customer Records Act (CAL. CIV. CODE §§ 1798.80, *et seq.*), violation of California's Unfair Competition Law (CAL. BUS. & PROF. CODE §§ 17200, *et seq.*), and declaratory and injunctive relief. Plaintiffs, on behalf of themselves and the Class, seek: (i) actual damages, economic damages, statutory damages, and nominal damages; (ii) punitive damages; (iii) fees and costs of litigation; (iv) injunctive relief,

including the adoption of reasonably sufficient practices to safeguard PII and PHI in Defendant's custody, care, and control in order to prevent incidents like the Data Breach from recurring in the future and for City of Hope to provide long-term, comprehensive identity theft protective services to Plaintiffs and Class Members; and (v) such other relief as the Court deems just and proper.

PARTIES

A. Plaintiffs

10. Plaintiff Joseph De Rivera is a resident and citizen of California, residing in Temecula, California.

11. Plaintiff Irwin Ojeda is a resident and citizen of California, residing in Palmdale, California.

12. Plaintiff d'Amileau Baulk is a resident and citizen of New Mexico, residing in Las Cruces, New Mexico.

B. Defendant

13. Defendant City of Hope National Medical Center d/b/a City of Hope is a non-profit California corporation headquartered at 1500 East Duarte Road, Duarte, California 91010.

JURISDICTION AND VENUE

14. This Court has original jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because at least member of the putative Class, as defined below, is a citizen of a state other than that of Defendant, there are more than 100 putative Class Members, and the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs.

15. This Court has personal jurisdiction over City of Hope because Defendant is a California corporation, maintains its principal place of business in Duarte, California, regularly conducts business in California, and has sufficient minimum contacts in California, such as to not offend traditional notions of fair play and substantial justice.

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

16. This Court has personal jurisdiction over the Plaintiffs because Plaintiffs either reside in this District or otherwise submit to the Court's jurisdiction.

17. Venue is proper in this District under 28 U.S.C. §§ 1391(b), (c), and (d) because City of Hope is a California corporation (and thus resides in this District), is headquartered in California, and a substantial part of the conduct giving rise to Plaintiffs' claims are resulting harms occurred in this District, including Defendant collecting or storing the PII and PHI of Plaintiffs and the putative Class Members.

FACTUAL BACKGROUND

A. City of Hope Collects, Stores, and Maintains Huge Amounts of Personally Identifiable Information and Protected Health Information.

18. City of Hope states that it is a "world-renowned pioneer in cancer research, treatment and prevention."[7] It treats patients across the United States through its "national footprint of cancer centers."[8] According to its most currently available annual report, in 2022, City of Hope provided care to over 131,000 patients and employs more than 11,000 individuals.[9]

19. To obtain City of Hope's healthcare services or as a condition of employment (or potential employment), patients and other persons—like Plaintiffs De Rivera, Ojeda, and Baulk—must provide their doctors, medical professionals, the human resources department, or Defendant directly with a wide array of highly sensitive information, including health and financial information. Because City of Hope regularly provides healthcare to over 100,000 patients annually and employs

[7] https://www.cityofhope.org/ (last visited Apr. 29, 2024).

[8] *Id.*

[9] 2022 Annual Report, CITY OF HOPE, *supra* note 1.

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

more than 11,000 persons, City of Hope's networks, files, and servers maintain in total at least several hundreds of thousands of persons' most private information.

20. City of Hope understands and acknowledges its cybersecurity obligations. Defendant's Notice of Privacy Practices admit it is "required by law to maintain the privacy of your protected health information ('PHI'), to provide you with notice of our legal duties and privacy practices with respect to your PHI, and to notify you in the event of a breach of your unsecured PHI."[10] Unless specifically carved out by City of Hope's privacy policy, Defendant admits that it "may use or disclose your PHI only when you give us permission to do so by written authorization."[11] Finally, City of Hope recognizes that certain patients' PHI within its systems is "Highly Confidential," for which "special privacy protections" under federal and state laws apply.[12]

21. Despite these strong proclaimed policies and approaches to patient privacy, City of Hope failed to adequately secure and safeguard its systems and networks from a foreseeable and preventable cyberattack. This conduct proximately resulted in the Data Breach and significant harm to Plaintiffs and the Class.

B. <u>The Three-Weeklong Data Breach Exposed Valuable PII and PHI</u>

22. City of Hope collected and maintained Plaintiffs' and the Class's PII and PHI in its computer systems, servers, and networks. In accepting, collecting, and maintaining Plaintiffs' and the Class's PII and PHI, City of Hope agreed that it would protect and safeguard that data by complying with state and federal laws and regulations and applicable industry standards. City of Hope was in possession of Plaintiffs' and the Class's PII and PHI before, during, and after the Data Breach.

[10] *Notice of Privacy Practices*, CITY OF HOPE, *supra* note 3.

[11] *See id.*

[12] *See id.*

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

23. According to City of Hope's Data Breach letters, around October 13, 2023, City of Hope first "became aware of suspicious activity on a subset of its systems."[13] Following an investigation with assistance from outside cybersecurity experts, City of Hope determined that the Data Breach occurred between September 19, 2023 and October 12, 2023.[14] In other words, the cyberattack went completely undetected for twenty-three days before City of Hope learned of the breach, during which time the bad actor had unfettered access to certain City of Hope's systems. City of Hope admits that PII and PHI was actually stolen during the Data Breach, confessing that the hacker "copied files."[15]

24. On December 14, 2023—two months after the Data Breach occurred—City of Hope says it "provided initial notice of the cybersecurity incident to potentially affected data subjects that could be readily notified via email without regard to the data subjects' state of residency."[16] More than three months later, on April 2, 2024—and ***over five months after the Data Breach occurred***—City of Hope then reported the Data Breach to various governmental agencies and attorneys general. City of Hope offers no explanation for this extreme delay.

25. Despite City of Hope's duties and commitments to safeguard sensitive and private information, City of Hope failed to follow industry-standard practices in securing Plaintiffs' and the Class Members' PII and PHI, as evidenced by the Data Breach.

---

[13] *See* Exhibit 1.

[14] *See id.*

[15] *See id.*

[16] James T. Kitchen, Letter to the Office of Attorney General, State of Maine (Apr. 2., 2024), *available at* https://apps.web.maine.gov/online/aeviewer/ME/40/1bb296e2-ea79-438c-b357-28ef738a0bf6/010c352d-c5df-4f98-85ce-7dea3b902a5c/document.html

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

26. In response to the Data Breach, City of Hope contends that it "immediately instituted mitigation measures to minimize any disruption to its operations" and later "implemented additional and enhanced safeguards" to protect its networks, systems, and data.[17] Although City of Hope failed to expand on what these purportedly "additional and enhanced safeguards" are, such policies and practices clearly should have been in place and fully operational *before* the Data Breach. Additionally, although City of Hope indicated that it notified federal law enforcement of the Data Breach, the Data Breach letters do not state whether the criminals responsible for the Data Breach have been identified or apprehended.

27. As of April 2, 2024, City of Hope reported to the Maine Attorney General's Office that the total number of persons affected by the Data Breach was 827,149.

28. City of Hope's Data Breach letters reveal that a treasure trove of information from Plaintiffs and the Class was stolen in the cyberattack, including, at least: names, email addresses, phone numbers, dates of birth, Social Security numbers, driver's licenses or other government identifications, financial details such as bank account numbers and credit card information, health insurance information, medical records and medical histories, including medical conditions.

29. Through the Notice of Data Breach letters, City of Hope also recognized the actual imminent harm and injury that flowed from the Data Breach and encouraged Data Breach victims to "remain vigilant to protect against potential fraud and identity theft by reviewing your account statements, monitoring your credit reports, and notifying your financial institutions of any potential suspicious activity."[18] Plaintiffs and the Class were only offered two years of complimentary identity monitoring

[17] *See* Exhibit 1.

[18] *Id.*

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

services through City of Hope's hand-picked vendor, Kroll. This offer does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the Data Breach involves PII that is difficult or even impossible to change, such as Social Security numbers and dates of birth. Further, the Data Breach exposed nonpublic, highly private information, including PHI, which is disturbing harm in of itself. Even with complimentary short-term identity monitoring services, the risk of identity theft and unauthorized use of Plaintiffs' and Class Members' PII and PHI is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

C. The Healthcare Sector Is Increasingly Susceptible to Data Breaches, Giving City of Hope Ample Notice That It Was a Likely Cyberattack Target

30. At all relevant times, City of Hope knew, or should have known, that the PII and PHI it was entrusted with was a prime target for malicious actors. Defendant knew this given the unique type and the significant volume of data on its networks, servers, and systems, comprising individuals' detailed and confidential personal information and, thus, the significant number of individuals who the exposure of the unencrypted data would harm.

31. As custodian of Plaintiffs' and Class Members' PII and PHI, City of Hope knew or should have known the importance of protecting their PII and PHI, and of the foreseeable consequences and harms to such persons if any data breach occurred.

32. City of Hope was on notice that the FBI has been long concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[19]

33. Defendant's security obligations were especially important due to the substantial increase of cyberattacks and data breaches in recent years, particularly those targeting healthcare businesses and other organizations like Defendant, which store and maintain large volumes of PII and PHI. These largescale cyberattacks are increasingly common and well-publicized. In 2023, a total of 725 largescale cyberattacks targeted hospitals, health systems, and healthcare records, affecting more than 133 million people—making 2023 the "worst-ever year for breached healthcare records."[20] With the surging number of such attacks targeting companies in the healthcare sector, City of Hope knew or should have known that it was at high risk of cyberattack and should have taken additional and stronger precautions and preemptive measures.

D. City of Hope Breached Its Duties to Plaintiffs and the Class Members, and Failed to Comply with Regulatory Requirements and Industry Practices.

34. Because Defendant was entrusted with PII and PHI at all times herein relevant, City of Hope owed to Plaintiffs and the Class a duty to exercise commercially reasonable methods and care in handling, using, maintaining, storing, and safeguarding the PII and PHI in its care, control, and custody, including by implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that occurred, and

[19] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 20, 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820.

[20] Steve Alder, *Security Breaches in Healthcare in 2023*, THE HIPAA JOURNAL (Jan. 31, 2024), https://www.hipaajournal.com/security-breaches-in-healthcare/.

to promptly detect and thwart attempts at unauthorized access to its networks and systems. Defendant also owed a duty to safeguard PII and PHI because it was on notice that it was handling highly valuable data and knew there was a significant risk it would be targeted by cybercriminals. Furthermore, City of Hope knew of the extensive, foreseeable harm that would ensue for the victims of a data breach, and therefore also owed a duty to reasonably safeguard that information.

35. Security standards commonly accepted among companies like City of Hope that store PII and PHI include, without limitation:

i. Maintaining a secure firewall configuration;

ii. Monitoring for suspicious or irregular traffic to servers or networks;

iii. Monitoring for suspicious credentials used to access servers or networks;

iv. Monitoring for suspicious or irregular activity by known users;

v. Monitoring for suspicious or unknown users;

vi. Monitoring for suspicious or irregular server requests;

vii. Monitoring for server requests for PII or PHI;

viii. Monitoring for server requests from virtual private networks (VPNs); and

ix. Monitoring for server requests for Tor exit nodes.

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

36. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity[21] and protection of PII which includes basic security standards applicable to all types of businesses.[22]

37. The FTC recommends that businesses:

i. Identify all connections to the computers where sensitive information is stored.

ii. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

iii. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

iv. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

v. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hacker attacks.

vi. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

---

[21] Start with Security: A Guide for Business, FTC (June 2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[22] Protecting Personal Information: A Guide for Business, FTC (Oct. 2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

vii. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

viii. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

ix. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business's network, the transmission should be investigated to make sure it is authorized.

38. As described further below, Defendant owed a duty to safeguard PII and PHI under several statutes, including the Federal Trade Commission Act, 15 U.S.C. § 45 (the "FTC Act") and as a covered entity under HIPAA, to ensure that all information it received, maintained, and stored was secure. These statutes were enacted to protect Plaintiffs and the Class Members from the type of conduct in which Defendant engaged, and the resulting harms Defendant proximately caused Plaintiffs and the Class Members.

39. Under the FTC Act, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard the PII and PHI of Plaintiffs and Class Members. Under HIPAA, 42 U.S.C. § 1320d, and its implementing regulations, 45 C.F.R. §§ 160, *et seq.*, Defendant had a duty to securely store and

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

maintain the PII and PHI of Plaintiffs and Class Members which was collected in conjunction with receiving medical services.

40. Defendant breached its duty to exercise reasonable care in protecting Plaintiffs' and Class Members' PII and PHI by failing to implement and maintain adequate data security measures to safeguard Plaintiffs' and Class Members' sensitive personal information, failing to encrypt or anonymize PII and PHI within its systems and networks, failing to monitor its systems and networks to promptly identify and thwart suspicious activity, failing to delete and purge PII and PHI no longer necessary for its provision of healthcare services to its patients and other persons, allowing unmonitored and unrestricted access to unsecured PII and PHI, and allowing (or failing to prevent) unauthorized access to, and exfiltration of, Plaintiffs' and Class Member's confidential and private information. Additionally, Defendant breached its duty by utilizing outdated and ineffectual data security measures which deviated from standard industry best practices at the time of the Data Breach. Through these actions, City of Hope also violated its duties under the FTC Act and HIPAA.

41. Defendant failed to prevent the Data Breach. Had City of Hope properly maintained and adequately protected its systems, servers, and networks, the Data Breach would not have occurred.

42. Additionally, the law imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of PII and PHI to Plaintiffs and Class Members so that they can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuses of their private information. City of Hope further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class Members. In so doing, Defendant actually and proximately caused and exacerbated the harm from the Data Breach and the injuries-in-fact of Plaintiffs and Class Members.

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

E. The Experiences of Plaintiffs De Rivera, Ojeda, and Baulk

43. Plaintiffs De Rivera, Ojeda, and Baulk each received notice of the Data Breach by letter from City of Hope dated April 2, 2024. At various relevant times, Plaintiffs De Rivera and Ojeda received healthcare services from City of Hope. In contrast, Baulk was never a City of Hope patient but did apply for a City of Hope job opening approximately ten years ago, suggesting the City of Hope Data Breach encompassed non-patients and other unrelated persons.

44. As a proximate result of the Data Breach, De Rivera, Ojeda, and Baulk will spend time for the foreseeable future and beyond dealing with its consequences and self-monitoring their accounts and credit reports to monitor potentially suspicious and fraudulent activity. This time will be lost forever and cannot be recaptured.

45. Following the Data Breach, Baulk received a notice from Experian on April 24, 2024 that certain of his personal information had been found on the dark web. Recently, Ojeda experienced fraudulent charges on his bank account exceeding $500. Additionally, in the months following the Data Breach, De Rivera has experienced a significant uptick in phishing emails, texts, and phone calls which request his personal information, such as bank account information or his Social Security number, which he believes may have resulted from the Data Breach. Ojeda has also seen a recent increase in spam phone calls, and now on average receives such calls about three times per week.

46. Baulk has lost sleep because his personal information was compromised in the Data Breach, the uncertainty surrounding how City of Hope came to possess his information in the first instance, and not knowing who stole his information or for what purpose. Similarly, the Data Breach has caused De Rivera anxiety and he fears "something bad" will happen now that his personal information has been compromised and that bad actors will utilize it for their personal gain. Likewise, the Data Breach has caused Ojeda anxiety, and feels both fearful and stressed that his private information was breached. This goes beyond allegations of mere worry or

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

inconvenience; it is exactly the sort of injury and harm to a data breach victim that the law contemplates and addresses.

47. De Rivera, Ojeda, and Baulk suffered actual injuries in the form of damages to and diminution in the value of their PII and PHI—a form of intangible property that was entrusted to City of Hope, which was compromised in and as a proximate result of the Data Breach.

48. De Rivera, Ojeda, and Baulk have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from their PII and PHI being obtained by unauthorized third parties and possibly cybercriminals.

49. De Rivera, Ojeda, and Baulk have a continuing interest in ensuring that their PII and PHI, which remains within City of Hope's possession and control, is protected and safeguarded against future data breaches or cybersecurity risks.

50. Defendant deprived De Rivera, Ojeda, and Baulk of the earliest opportunity to guard themselves against the Data Breach's harmful effects by failing to promptly notify them about it. Instead, ***City of Hope waited over five months***, without any explanation whatsoever.

F. Plaintiffs De Rivera, Ojeda, and Baulk and the Class Suffered Actual and Impending Injuries Resulting from the Data Breach

51. As a proximate result of Defendant's completely unreasonable security practices, identity thieves now possess the sensitive PII and PHI of De Rivera, Ojeda, Baulk, and the Class. That information is extraordinarily valuable on the black market and incurs direct costs to De Rivera, Ojeda, Baulk, and the Class. On the dark web—an underground internet black market—criminals openly buy and sell stolen PII and PHI to create "identity kits" worth up to $2,000 each that can be used to create fake IDs, gain access to bank accounts, social media accounts, and credit cards, file false

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

insurance claims or tax returns, or rack up other kinds of expenses.[23] And, "[t]he damage to affected [persons] may never be undone."[24]

52. Unlike the simple credit-card breaches at retail merchants, these damages cannot be avoided by canceling and reissuing plastic cards or closing an account. Identity theft is far more pernicious than credit card fraud. Criminals' ability to open entirely new accounts—not simply prey on existing ones—poses far more dangerous problems. Identity thieves can retain the stolen information for years until the controversy has receded because victims may become less vigilant in monitoring their accounts as time passes. Then, at any moment, the thief can take control of a victim's identity, resulting in thousands of dollars in losses and lost productivity. The U.S. Department of Justice has reported that in 2021, identity theft victims spent on average about four hours to resolve problems stemming therefrom and that the average financial loss experienced by an identity theft victim was $1,160 per person.[25] Additionally, about 80% of identity theft victims reported some form of emotional distress resulting from the incident.[26]

53. As a consequence of the Data Breach, Plaintiffs' and Class Members' credit profiles can be destroyed before they even realize what happened, and they may be unable to legitimately borrow money, obtain credit, or open bank accounts. Plaintiffs and Class Members can be deprived of legitimate tax refunds or, worse yet,

---

[23] Nick Culbertson, *Increased Cyberattacks on Healthcare Institutions Shows the Need for Greater Cybersecurity* (Jun. 7, 2021), FORBES, https://www.forbes.com/sites/forbestechcouncil/2021/06/07/increased-cyberattacks-on-healthcare-institutions-shows-the-need-for-greater-cybersecurity/?sh=ca928c05650d.

[24] *Id.*

[25] Erika Harrell and Alexandra Thompson, Victims of Identity Theft, 2021, U.S. DEPARTMENT OF JUSTICE, OFFICE OF JUSTICE PROGRAMS, BUREAU OF JUSTICE STATISTICS (Oct. 2023), *available at* https://bjs.ojp.gov/document/vit21.pdf.

[26] *Id.*

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

may face state or federal tax investigations due to fraud committed by an identity thief. And even the simple preventive step of adding oneself to a credit-fraud watch list to guard against these consequences substantially impairs Plaintiffs' and Class Members' ability to obtain additional credit. In fact, many experts advise victims to place a freeze on all credit accounts, making it impossible to rent a car, get student loans, buy or rent big-ticket items, or complete a major new car or home purchase.

54. Cybercriminals sell health information at a far higher premium than stand-alone PII. This is because health information enables thieves to go beyond traditional identity theft and obtain medical treatments, purchase prescription drugs, submit false bills to insurance companies, or even undergo surgery under a false identity.[27] The shelf life for this information is also much longer—while individuals can update their credit card numbers, they are less likely to change their health insurance information. When medical identity theft occurs, the associated costs to victims can be exorbitant. According to a 2015 study, at least 65% of medical identity theft victims had to "pay an average of $13,500 to resolve the crime."[28]

55. City of Hope's Data Breach notices to affected persons do not provide adequate remediation and compensation for its wrongful conduct and actions described herein. Therein, City of Hope says that it is "deeply sorry" for the incident, yet only offered affected individuals two years of complimentary identity protection service through its hand-picked vendor, Kroll.

[27] Medical Identity Theft: FAQs for Health Care Providers and Health Plans, FTC, *available at* https://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faq-health-care-health-plan.pdf.

[28] Justin Klawans, *What is medical identity theft and how can you avoid it?*, THE WEEK (Aug. 2, 2023), https://theweek.com/feature/briefing/1025328/medical-identity-theft-how-to-avoid.

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

CLASS ACTION ALLEGATIONS

56. Pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of the following nationwide class (the "Nationwide Class" or the "Class"):

> All persons whose PII or PHI was compromised in the Data Breach discovered by City of Hope on or about October 13, 2023, including all persons who were sent a notice of the Data Breach (and each person a "Class Member").

57. Within the Nationwide Class, there is one subclass (the "California Subclass") defined as follows:

> All persons residing in the State of California whose PII or PHI was compromised in the Data Breach discovered by City of Hope on or about October 13, 2023, including all persons who were sent a notice of the Data Breach (and each person a "California Subclass Member").

58. Excluded from the Nationwide Class and the California Subclass are governmental entities, City of Hope, any entity in which City of Hope has a controlling interest, and City of Hope's officers, directors, affiliates, legal representatives, co-conspirators, successors, subsidiaries, and assigns. Also excluded from the Nationwide Class and the California Subclass are any judges, justices, or judicial officers presiding over this matter and the members of their immediate families and judicial staff.

59. This action is brought and may be properly maintained as a class action pursuant to Federal Rule of Civil Procedure 23(b)(2) and 23(b)(3), and satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of these rules.

60. ***Numerosity Under Rule 23(a)(1).*** The Nationwide Class and the California Subclass are so numerous that the individual joinder of all members is impracticable, and the disposition of the claims of all members of the Nationwide Class and the California Subclass in a single action will provide substantial benefits

to the parties and the Court. Although the precise number of members of the Nationwide Class and California Subclass are unknown to Plaintiffs at this time, on information and belief, the proposed Nationwide Class contains at least 827,149 individuals, as reported to the Maine Attorney General. On information and belief and given the size of the Nationwide Class, the proposed California Subclass contains at least tens of thousands of individuals. Discovery will reveal, through City of Hope's records, the actual number of members of the Nationwide Class and California Subclass.

61. ***Commonality Under Rule 23(a)(2).*** Common legal and factual questions exist that predominate over any questions affecting only individual members of the Nationwide Class and California Subclass. These common questions, which do not vary among members of the Nationwide Class or California Subclass, and which may be determined without reference to any Nationwide Class or California Subclass member's individual circumstances, include, but are not limited to:

(a) Whether Defendant knew or should have known that its computer systems and networks were vulnerable to unauthorized third-party access or a cyberattack;

(b) Whether Defendant failed to utilize and maintain adequate and reasonable security and preventive measures to ensure that its computer systems and networks were protected;

(c) Whether Defendant failed to take available steps to prevent and stop the Data Breach from occurring;

(d) Whether Defendant owed a legal duty to Plaintiffs and Class Members to protect their PII and PHI;

(e) Whether Defendant breached any duty to protect the PII or PHI of Plaintiffs and Class Members by failing to exercise due care in protecting their sensitive and private information;

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

(f) Whether Defendant provided timely, accurate, and sufficient notice of the Data Breach to Plaintiffs and the Class Members;

(g) Whether Plaintiffs and Class Members have been damaged by the wrongs alleged and are entitled to actual, statutory, or other forms of damages and other monetary relief; and

(h) Whether Plaintiffs and Class Members are entitled to injunctive or equitable relief, including restitution.

62. ***Typicality Under Rule 23(a)(3).*** Plaintiffs' claims are typical of the claims of the Nationwide Class and California Subclass. De Rivera, Ojeda, and Baulk, like all proposed members of the Class and California Subclass, had their PII or PHI compromised in the Data Breach. City of Hope's uniformly unlawful course of conduct injured De Rivera, Ojeda, Baulk, Class Members, and California Subclass Members in the same wrongful acts and practices. Likewise, De Rivera, Ojeda, Baulk, and other Class Members and California Subclass Members must prove the same facts in order to establish the same claims.

63. ***Adequacy of Representation Under Rule 23(a)(4).*** De Rivera, Ojeda, and Baulk are adequate representatives of the Nationwide Class and California Subclass because they are Nationwide Class Members, De Rivera and Ojeda are members of the California Subclass, and their interests do not conflict with the interests of the Nationwide Class or California Subclass. De Rivera, Ojeda, and Baulk have retained counsel competent and experienced in complex litigation, data breach cases, and consumer protection class action matters such as this action, and De Rivera, Ojeda, and Baulk and their counsel intend to vigorously prosecute this action for the Nationwide Class's and California Subclass's benefit and have the resources to do so. De Rivera, Ojeda, and Baulk and their counsel have no interests adverse to those of the other members of the Nationwide Class or California Subclass.

64. ***Predominance and Superiority.*** A class action is superior to all other available methods for the fair and efficient adjudication of this controversy because

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

individual litigation of each Nationwide Class and California Subclass Member's claim is impracticable. The damages, harm, and losses suffered by the individual members of the Nationwide Class and California Subclass will likely be small relative to the burden and expense of individual prosecution of the complex litigation necessitated by City of Hope's wrongful conduct. Even if each Nationwide Class and California Subclass Member could afford individual litigation, the Court system could not. It would be unduly burdensome if tens of thousands of individual cases or more proceeded. Individual litigation also presents the potential for inconsistent or contradictory judgments, the prospect of a race to the courthouse, and the risk of an inequitable allocation of recovery among those individuals with equally meritorious claims. Individual litigation would increase the expense and delay to all parties and the Courts because it requires individual resolution of common legal and factual questions. By contrast, the class action device presents far fewer management difficulties and provides the benefit of a single adjudication, economies of scale, and comprehensive supervision by a single court.

65. As a result of the foregoing, class treatment under Federal Rule of Civil Procedure 23 is appropriate.

FIRST CLAIM FOR RELIEF
Negligence
(On Behalf of Plaintiffs and the Nationwide Class)

66. Plaintiffs incorporate by reference and reallege paragraphs 1-55 as if fully set forth herein.

67. In the ordinary course of providing healthcare services to its patients and other individuals and employing its staff, Defendant solicited, gathered, and stored the PII and PHI of Plaintiffs and Class Members. Because Defendant was entrusted with such PII and PHI at all times herein relevant, City of Hope owed to Plaintiffs and the Class a duty to exercise commercially reasonable methods and care in handling, using, maintaining, storing, and safeguarding the PII and PHI in its care, control, and

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

custody, including by implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that occurred, and to promptly detect and thwart attempts at unauthorized access to its networks and systems. This duty arose independently from any contract.

68. Defendant knew, or should have known, of the risks inherent in collecting and storing massive amounts of PII and PHI, including the importance of adequate data security and the high frequency of ransomware attacks and well-publicized data breaches both generally and the increasing rate of cybercriminals specifically targeting the healthcare industry, like Defendant. City of Hope owed a duty of care to Plaintiffs and Class Members because it was foreseeable that City of Hope's failure to adequately safeguard their PII and PHI in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that sensitive information. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and the Class's PII and PHI by failing to limit access to this information to unauthorized third parties and by not properly supervising both the way the PII and PHI was stored, used, and exchanged, and those in its employ responsible for such tasks.

69. Defendant owed to Plaintiffs and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII and PHI. City of Hope also owed a duty to timely and accurately disclose to Plaintiffs and Class Members the scope, nature, and circumstances of the Data Breach. This duty is required and necessary for Plaintiffs and the Class to take appropriate measures to protect their PII and PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

70. Defendant also had a common law duty to prevent foreseeable harm to others. Defendant had full knowledge of the sensitivity and high value of the PII and PHI that it stored and the types of foreseeable harm and injury-in-fact that Plaintiffs and Class Members could and would suffer if that PII and PHI were wrongfully

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

disclosed, leaked, accessed, or exfiltrated. City of Hope's conduct created a foreseeable and unreasonable risk of harm to Plaintiffs and Class Members, who were the foreseeable victims of City of Hope's inadequate data security practices.

71. Defendant violated its duty to implement and maintain reasonable security procedures and practices, including through its failure to adequately restrict access to its file systems and networks that held hundreds of thousands of individuals' PII and PHI or encrypt or anonymize such data. City of Hope's duty included, among other things, designing, maintaining, and testing City of Hope's information security controls to ensure that PII and PHI in its possession was adequately secured by, for example, encrypting or anonymizing sensitive personal information, installing intrusion detection and deterrent systems and monitoring mechanisms, and using access controls to limit access to sensitive data.

72. City of Hope's duty of care also arose by operation of statute, as follows:

a. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard the PII and PHI of Plaintiffs and Class Members; and

b. Pursuant to HIPAA, 42 U.S.C. § 1320d, and its implementing regulations, 45 C.F.R. §§ 160, *et seq.*, Defendant had a duty to securely store and maintain the PII and PHI of Plaintiffs and Class Members which was collected in conjunction with receiving healthcare services. Additionally, the HIPAA Breach Notification Rule, 45 C.F.R. § 164.400-414, required Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

73. These statutes—the FTC Act and HIPAA—were enacted to protect Plaintiffs and the Class Members from the type of wrongful conduct in which Defendant engaged.

74. Defendant breached its duty to exercise reasonable care in protecting Plaintiffs' and Class Members' PII and PHI by failing to implement and maintain

adequate data security measures to safeguard Plaintiffs' and Class Members' sensitive personal information, failing to encrypt or anonymize PII and PHI within its systems and networks, failing to monitor its systems and networks to promptly identify and thwart suspicious activity, failing to delete and purge PII and PHI no longer necessary for its provision of healthcare services to its patients, other persons, and persons within its employ, allowing unmonitored and unrestricted access to unsecured PII and PHI, and allowing (or failing to prevent) unauthorized access to, and copying and exfiltration of, Plaintiffs' and Class Members' confidential and private information. Additionally, Defendant breached its duty by utilizing outdated and ineffectual data security measures which deviated from standard industry best practices at the time of the Data Breach. Through these actions, City of Hope also violated its duties under the FTC Act and HIPAA.

75. The law imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of PII and PHI to Plaintiffs and Class Members so that they can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuses of their private information. City of Hope further breached its duties by failing to provide such reasonably timely notice of the Data Breach to Plaintiffs and Class Members, including by violating the HIPAA Breach Notification Rule. In so doing, Defendant actually and proximately caused and exacerbated the harm from the Data Breach and the injuries-in-fact of Plaintiffs and Class Members. Timely disclosure was necessary so that Plaintiffs and Class Members could, among other things: (i) purchase identity theft protection, monitoring, and recovery services; (ii) flag asset, credit, and tax accounts for fraud; (iii) purchase or otherwise obtain credit reports; (iv) place or renew fraud alerts on a quarterly basis; (v) closely monitor loan data and public records; and (vi) take other meaningful steps to protect themselves and attempt to avoid or recover from identity theft and other harms.

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

76. As stated in City of Hope's 2022 Annual Report, Defendant held assets valued at almost $2.6 billion and collected revenues topping $3.3 billion, and accordingly had the financial and personnel resources necessary to prevent the Data Breach. City of Hope nevertheless failed to adopt reasonable data security measures, in breach of the duties it owed to Plaintiffs and Class Members.

77. Plaintiffs and Class Members had no ability to protect their PII and PHI once it was in City of Hope's possession and control. City of Hope was in an exclusive position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

78. But for Defendant's breach of its duty to adequately protect Class Members' PII and PHI, Class Members' PII and PHI would not have been stolen. As a result of City of Hope's negligence, Plaintiffs and Class Members suffered and will continue to suffer the various types of damages alleged herein. There is a temporal and close causal connection between City of Hope's failure to implement adequate data security measures, the Data Breach, and the harms suffered by Plaintiffs and Class Members.

79. As a direct and traceable result of Defendant's negligence, Plaintiffs and the Class have suffered or will suffer an increased and impending risk of fraud, identity theft, damages, embarrassment, humiliation, frustration, emotional distress, and lost time and out-of-pocket costs to mitigate and remediate the effects of the Data Breach. These harms to Plaintiffs and the Class include, without limitation: (i) loss of the opportunity to control how their personal information is used; (ii) diminution in the value and use of their personal information entrusted to Defendant; (iii) the compromise and theft of their personal information; (iv) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and unauthorized use of financial accounts; (v) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including increased costs to use credit, credit scores, credit reports, and assets; (vi) unauthorized use of

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

compromised personal information to open new financial and other accounts; (vii) continued risk to their personal information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the personal information in its possession; and (viii) future costs in the form of time, effort, and money they will expend to prevent, detect, contest, and repair the adverse effects of their personal information being stolen in the Data Breach.

80. Defendant's negligence was gross, willful, wanton, and warrants the imposition of punitive damages given the clear foreseeability of a hacking incident, the extreme sensitivity of the private information under Defendant's care, and its failure to take adequate remedial steps, including prompt notification of the victims, following the Data Breach.

81. Plaintiffs and Class Members are entitled to all forms of monetary compensation set forth herein, including monetary payments to provide adequate long-term identity protection services. Plaintiffs and Class Members are also entitled to the injunctive relief sought herein.

SECOND CLAIM FOR RELIEF
Negligence *Per Se*
(On Behalf of Plaintiffs and the Nationwide Class)

82. Plaintiffs incorporate by reference and reallege paragraphs 1-55 as if fully set forth herein.

83. Pursuant to the FTC Act, 15 U.S.C. § 45, City of Hope had a duty to maintain fair and adequate computer systems and data security practices to safeguard Plaintiffs' and the Class's PII and PHI.

84. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers' PII. The FTC publications and orders promulgated pursuant to the

FTC Act also form part of the basis of City of Hope's duty to protect Plaintiffs' and the Class Members' PII and PHI.

85. Pursuant to HIPAA, 42 U.S.C. §§ 1302, *et seq.*, City of Hope also owed Plaintiffs and Class Members a duty to provide adequate data security practices and to safeguard their PII and PHI.

86. City of Hope's duty to use reasonable care in protecting confidential and sensitive data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII and PHI.

87. City of Hope violated its duties under Section 5 of the FTC Act and HIPAA by failing to use reasonable or adequate data security practices and measures to protect Plaintiffs' and the Class's PII and PHI and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI that City of Hope collected and stored and the foreseeable consequences of a cybersecurity data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

88. The harm that has occurred is the type of harm the FTC Act and HIPAA are intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

89. But for Defendant's wrongful and negligent breach of the duties owed to Plaintiffs and Class Members, Plaintiffs and the Class Members would not have been injured.

90. The injuries and harms suffered by Plaintiffs and the Class Members were the reasonably foreseeable result of Defendant's breach of its duties. City of Hope knew or should have known that it was failing to meet its duties and that its

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

breach would cause Plaintiffs and the Class Members to suffer the foreseeable harms associated with the exposure of their PII and PHI.

91. Defendant's various violations and its failure to comply with the applicable laws and regulations referenced above constitutes negligence *per se*.

92. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII and PHI; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII and PHI, entitling them to damages in an amount to be proven at trial.

93. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their PII and PHI, which remain in City of Hope's possession and is subject to further unauthorized disclosures so long as City of Hope fails to undertake appropriate and adequate measures to protect the PII and PHI in its continued possession.

THIRD CLAIM FOR RELIEF
Invasion of Privacy
(On Behalf of Plaintiffs and the Nationwide Class)

94. Plaintiffs incorporate by reference and reallege paragraphs 1-55 as if fully set forth herein.

95. Plaintiffs and Class Members have a legally protected privacy interest in their PII and PHI, which is and was collected, stored, and maintained by City of Hope, and they are entitled to the reasonable and adequate protection of their PII and PHI against foreseeable unauthorized access, as occurred with the Data Breach.

96. Plaintiffs and Class Members reasonably expected that Defendant would protect and secure their PII and PHI from unauthorized parties and that their private

information would not be accessed, exfiltrated, and disclosed to any unauthorized parties or for any improper purpose.

97. City of Hope unlawfully invaded the privacy rights of Plaintiffs and Class Members by engaging in the wrongful conduct described above, including by failing to protect their PII and PHI by permitting unauthorized third parties to access, exfiltrate, copy, and view this private information. Likewise, City of Hope further invaded the privacy rights of Plaintiffs and Class Members, and permitted cybercriminals to invade the privacy rights of Plaintiffs and Class Members, by unreasonably and intentionally delaying disclosure of the Data Breach, and failing to properly identify what PII and PHI had been accessed, exfiltrated, copied, and viewed by unauthorized third parties.

98. This invasion of privacy resulted from Defendant's failure to properly secure and maintain Plaintiffs' and the Class Members' PII and PHI, leading to the foreseeable unauthorized access, exfiltration, and disclosure of this unguarded data.

99. Plaintiffs' and the Class Members' PII and PHI is the type of sensitive, personal information that one normally expects will be protected from exposure by the very entity charged with safeguarding it. Further, the public has no legitimate concern in Plaintiffs' and the Class Members' PII and PHI, and such private information is otherwise protected from exposure to the public by various statutes, regulations, and other laws.

100. The disclosure of Plaintiffs' and the Class Members' PII and PHI to unauthorized parties is substantial and unreasonable enough to be legally cognizable and is highly offensive to a reasonable person.

101. City of Hope's willful and reckless conduct which permitted unauthorized access, exfiltration and disclosure of Plaintiffs' and the Class Members' sensitive, PII and PHI is such that it would cause serious mental injury, shame, embarrassment, or humiliation to people of ordinary sensibilities.

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

102. The unauthorized access, exfiltration, and disclosure of Plaintiffs' and the Class Members' PII and PHI was without their consent, and in violation of various statutes, regulations, and other laws.

103. As a result of the invasion of privacy caused by Defendant, Plaintiffs and the Class Members suffered and will continue to suffer damages and injuries as set forth herein.

104. Plaintiffs and the Class Members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution, injunctive relief, reasonable attorneys' fees and costs, and any other relief that the Court deems just and proper.

FOURTH CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class)

105. Plaintiffs incorporate by reference and reallege paragraphs 1-55 as if fully set forth herein.

106. This claim is pleaded in the alternative to Plaintiffs' unjust enrichment and quasi-contract claim, *infra*.

107. Through their course of conduct, Plaintiffs and the Class Members entered into implied contracts with City of Hope under which City of Hope agreed to safeguard and protect their confidential and private PII and PHI and to timely and accurately notify Plaintiffs and Class Members if their information had been breached and compromised.

108. City of Hope acquired, stored, and maintained the PII and PHI of Plaintiffs and the Class that it received either directly from them or that City of Hope otherwise received from other third parties.

109. Plaintiffs and Class Members were required to provide, or authorize the transfer of, their private information and health information in order for City of Hope to provide its healthcare services, or for purposes of employment. Plaintiffs and Class

Members paid money, or money was paid on their behalf, or provide services to City of Hope in exchange for such services or employment.

110. City of Hope solicited, offered, and invited Class Members to provide their private information and health information as part of City of Hope's regular business practices. Plaintiffs and Class Members accepted City of Hope's offers and provided their private information and health information to City of Hope.

111. City of Hope accepted possession of Plaintiffs' and Class Members' PII and PHI for the purpose of providing healthcare services or employment to Plaintiffs and Class Members.

112. When Plaintiffs and Class Members paid money and provided their PII and PHI to City of Hope and their healthcare providers, either directly or indirectly, in exchange for healthcare services, they entered into implied contracts with their healthcare providers and their business associates, including City of Hope, and intended and understood that PII and PHI would be adequately safeguarded as part of that service. Alternatively, Plaintiffs and Class Members are the intended third-party beneficiaries of data protection agreements entered into between City of Hope and its healthcare provider clients.

113. City of Hope's implied promise of confidentiality to Plaintiffs and Class Members includes consideration beyond those pre-existing general duties owed under the FTC Act, HIPAA, or other state or federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

114. City of Hope's implied promises include but are not limited to: (a) taking steps to ensure that any agents who are granted access to PII and PHI also protect the confidentiality of that data; (b) taking steps to ensure that the information that is placed in the control of its agents is restricted and limited to achieve an authorized medical purpose; (c) restricting access to qualified and trained agents; (d) designing and implementing appropriate retention policies to protect the information against

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

criminal data breaches; (e) applying or requiring proper encryption; (f) multifactor authentication for access; and (g) other steps to protect against foreseeable data breaches.

115. Defendant's implied promises to safeguard Plaintiffs' and Class Members' PII and PHI are evidenced by, *e.g.*, representations in City of Hope's Notice of Privacy Practices described above. The mutual understanding and intent of Plaintiffs and Class Members on the one hand, and City of Hope on the other, is further demonstrated by their conduct and course of dealing.

116. Plaintiffs and the Class Members would not have entrusted their PII and PHI to City of Hope in the absence of such an implied contract. Had City of Hope disclosed to Plaintiffs and the Class (or their physicians and other healthcare providers) that it did not have adequate computer systems and security practices to secure sensitive data, Plaintiffs and the other Class Members (or their physicians and healthcare providers) would not have provided their PII and PHI to City of Hope.

117. City of Hope recognized that Plaintiffs' and Class Members' PII and PHI is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiffs and the other Class Members.

118. Plaintiffs and the Class Members fully and adequately performed their obligations under the implied contracts with City of Hope.

119. City of Hope breached the implied contracts it made with Plaintiffs and the Class Members by failing to take reasonable measures to safeguard their PII and PHI as described herein, as well as by failing to provide accurate, adequate, and timely notice to them that their PII and PHI was compromised as a result of the Data Breach.

120. As a direct and proximate result of City of Hope's wrongful conduct, Plaintiffs and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial, or alternatively, nominal damages. Plaintiffs and Class Members are also entitled to injunctive relief requiring City of Hope to strengthen its data security systems, submit to future audits of those systems, and

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

provide adequate long-term credit monitoring and identity theft protection services to all persons affected by the Data Breach.

FIFTH CLAIM FOR RELIEF
Unjust Enrichment / Quasi-Contract
(On Behalf of Plaintiffs and the Nationwide Class)

121. Plaintiffs incorporate by reference and reallege paragraphs 1-55 as if fully set forth herein.

122. This claim is pleaded in the alternative to Plaintiffs' breach of implied contract claim, *supra*.

123. A monetary benefit was directly and indirectly conferred upon Defendant through its receipt of Plaintiffs' and Class Members' PII and PHI, which City of Hope used to facilitate the provision of healthcare services or for purposes of employment. City of Hope appreciated or had knowledge of these benefits conferred upon it by Plaintiffs and the Class.

124. Under principles of equity and good conscience, Defendant should not be permitted to retain the full monetary value of the benefits because City of Hope failed to adequately protect Plaintiffs' and Class Members' PII and PHI.

125. Plaintiffs and the Class Members have no adequate remedy at law. City of Hope continues to retain their PII and PHI while exposing this sensitive and private information to a risk of future data breaches while in Defendant's possession. Defendant also continues to derive a financial benefit from using Plaintiffs' and Class Members' PII and PHI.

126. As a direct and proximate result of Defendant's wrongful conduct, Plaintiffs and the Class Members have suffered various types of damages alleged herein.

127. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds received by it because of its misconduct described herein and the Data Breach.

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

SIXTH CLAIM FOR RELIEF
California Confidentiality of Medical Information Act,
CAL. CIV. CODE §§ 56, *et seq.*
(On Behalf of Plaintiffs De Rivera and Ojeda and the California Subclass)

128. Plaintiffs De Rivera and Ojeda incorporate by reference and reallege paragraphs 1-55 as if fully set forth herein.

129. CAL. CIV. CODE § 56.10(a) provides that "[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization[.]"

130. City of Hope is a "provider of health care," as defined in CAL. CIV. CODE § 56.05(p), and is therefore subject to the requirements of the California Confidentiality of Medical Information Act, CAL. CIV. CODE §§ 56, *et seq.* (the "CMIA").

131. Plaintiffs De Rivera and Ojeda and California Subclass Members are "patients," as defined by the California CMIA to whom "medical information" in the possession of Defendant pertains, as defined in CAL. CIV. CODE §§ 56.05(m) and (j).

132. As "patients" within the meaning of the California CMIA, Plaintiffs De Rivera and Ojeda and California Subclass Members had their "medical information" created, maintained, preserved, and stored on Defendant's computer networks at the time of the City of Hope Data Breach.

133. Defendant disclosed medical information pertaining to members of the proposed California Subclass to unauthorized persons without first obtaining their consent, in violation of CAL. CIV. CODE §§ 56.10(a) and 56.11.

134. Through inadequate security, Defendant allowed an unauthorized third party to gain access to, view, copy, and/or download the medical information of Plaintiffs De Rivera and Ojeda and the California Subclass. Defendant's negligence resulted in the release of individually identifiable medical information pertaining to

members of the California Subclass to unauthorized persons and the breach of the confidentiality of that information. Defendant's negligent failure to maintain or preserve medical information pertaining to members of the California Subclass in a manner that preserved the confidentiality of the information contained therein violates CAL. CIV. CODE § 56.101(a).

135. Plaintiffs De Rivera and Ojeda and the California Subclass Members' medical information that was the subject of the City of Hope Data Breach included "electronic medical records" or "electronic health records" as referenced by CAL. CIV. CODE § 56.101(d) and defined by 42 U.S.C. § 17921(5).

136. Defendant also violated CAL. CIV. CODE § 56.101(b) through its failure to protect and preserve the integrity of Defendant's electronic health record systems and electronic medical records systems. Plaintiffs De Rivera and Ojeda and California Subclass Members' PHI was viewed by unauthorized individuals as a direct and proximate result of Defendant's violations of CAL. CIV. CODE § 56.101(b)(1)(A).

137. Defendant is further liable for any further disclosures of Plaintiffs De Rivera's and Ojeda's and California Subclass Members' medical information pursuant to CAL. CIV. CODE §§ 56.13 and 56.14.

138. As a direct and proximate result of Defendant's conduct and illegal disclosure and negligent release of medical information in violation of CAL. CIV. CODE §§ 56.10 and 56.101, Plaintiffs De Rivera and Ojeda and the California Subclass were injured and have suffered (and will continue to suffer) damages. Plaintiffs De Rivera and Ojeda and the California Subclass therefore seek relief under CAL. CIV. CODE §§ 56.35 and 56.36, including, but not limited to, actual damages, nominal statutory damages of $1,000, civil penalties, punitive damages, injunctive and equitable relief, and/or attorneys' fees and costs.

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

SEVENTH CLAIM FOR RELIEF

California Customer Records Act, CAL CIV. CODE §§ 1798.80, *et seq.*

(On Behalf of Plaintiffs De Rivera and Ojeda and the California Subclass)

139. Plaintiffs De Rivera and Ojeda incorporate by reference and reallege paragraphs 1-55 as if fully set forth herein.

140. "[T]o ensure that personal information about California residents is protected," the California legislature enacted CAL CIV. CODE § 1798.81.5, which requires that any business that "owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

141. Defendant is a business that owns, maintains, or licenses personal information, within the meaning of CAL CIV. CODE § 1798.81.5, about Plaintiffs De Rivera and Ojeda and California Subclass Members.

142. City of Hope violated CAL CIV. CODE § 1798.81.5 by failing to implement reasonable measures to protect California Subclass Members' PII and PHI.

143. Businesses that own or license computerized data that includes personal information are required to notify California residents when their PII or PHI has been acquired (or has reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." CAL CIV. CODE § 1798.82. Among other requirements, the security breach notification must include "the types of personal information that were or are reasonably believed to have been the subject of the breach." CAL CIV. CODE § 1798.82.

144. Defendant is a business that owns or licenses computerized data that includes personal information as defined by CAL CIV. CODE § 1798.82.

145. Plaintiffs De Rivera's and Ojeda's and California Subclass Members' PII or PHI includes personal information identified in CAL CIV. CODE § 1798.82(h) such as their names, Social Security numbers, driver's licenses or other government identifications, financial details (including bank account numbers and credit card details), health insurance information, and medical information, and is thereby covered by CAL CIV. CODE § 1798.82.

146. Plaintiffs De Rivera and Ojeda and the California Subclass Members are "customers" within the meaning of CAL CIV. CODE § 1798.80(c), as their personal information was provided to Defendant for the purpose of obtaining services or products.

147. The Data Breach constituted a breach of City of Hope's security systems, networks, and servers.

148. Because City of Hope reasonably believed that Plaintiffs De Rivera's and Ojeda's and California Subclass Members' PII or PHI was acquired by unauthorized persons during the Data Breach, Defendant had an obligation to disclose the data breach in a timely and accurate fashion as mandated by CAL CIV. CODE § 1798.82.

149. City of Hope unreasonably delayed informing Plaintiffs De Rivera and Ojeda and the California Subclass Members about the breach of security of their PII or PHI after it knew the breach had occurred. By way of example, City of Hope sent both Plaintiffs De Rivera and Ojeda a Notice of Data Breach letters dated April 2, 2024—more than five months after Defendant first discovered that the Data Breach occurred.

150. Upon information and belief, no law enforcement agency instructed Defendant that notification to California Subclass Members would impede an investigation. Nor do the Notice of Data Breach letters sent to California Subclass Members provide any explanation whatsoever for the extreme delay between City of

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

Hope's discovery of the Data Breach and its sending notifications to all affected persons.

151. Thus, by failing to disclose the Data Breach in a timely and accurate manner, the Defendant also violated CAL CIV. CODE § 1798.82.

152. Pursuant to CAL CIV. CODE § 1798.84, "[a]ny waiver of a provision of this title is contrary to public policy and is void and unenforceable," "[a]ny customer injured by a violation of this title may institute a civil action to recover damages," and "[a]ny business that violates, proposed to violate, or has violated this title may be enjoined."

153. As a direct and proximate result of Defendant's violations of CAL CIV. CODE §§ 1798.81.5 and 1798.82, Plaintiffs De Rivera and Ojeda and California Subclass Members were (and continue to be) injured and suffered (and will continue to suffer) damages, as described above.

154. Plaintiffs De Rivera and Ojeda and California Subclass Members seek relief under CAL CIV. CODE § 1798.84, including, but not limited to, actual damages, any applicable statutory damages, and equitable and injunctive relief.

EIGHTH CLAIM FOR RELIEF

California Unfair Competition Law, CAL. BUS. & PROF. CODE §§ 17200, *et seq.*
(On Behalf of Plaintiffs De Rivera and Ojeda and the California Subclass)

155. Plaintiffs De Rivera and Ojeda incorporates by reference and reallege paragraphs 1-55 as if fully set forth herein.

156. Defendant violated California's Unfair Competition Law, CAL. BUS. & PROF. CODE §§ 17200, *et seq.* (the "UCL"), by engaging in unlawful, unfair, or fraudulent business acts and practices that constitute acts of "unfair competition" as defined in the UCL with respect to its conduct and actions with and towards Plaintiffs De Rivera and Ojeda and the California Subclass.

157. Defendant's actions as alleged herein in this Class Action Complaint constitute an "unlawful" practice as encompassed by the UCL because Defendant's

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

actions: (a) violated the California Consumer Records Act, CAL. CIV. CODE §§ 1798.80, *et seq.*, (b) violated the California CMIA, CAL. CIV. CODE §§ 56, *et seq.* (c) constituted negligence and negligence *per se*; and (d) violated federal law and regulations, including the FTC Act and HIPAA.

158. Defendant's actions as alleged in this Class Action Complaint also constitute an "unfair" practice as encompassed by the UCL because they offend established public policy and are immoral, unethical, oppressive, unscrupulous, and substantially injurious. The harm caused by Defendant's wrongful conduct outweighs any utility of such conduct and has caused—and will continue to cause—substantial injury to the California Subclass. There were ample reasonably available alternatives that would have furthered Defendant's legitimate business practices, including using industry-standard technologies to protect data (e.g., two-factor authorization, effective encryption and anonymization, software patches, and the purging of data no longer necessary for Defendant's healthcare services). Defendant also unreasonably delayed in notifying Plaintiffs De Rivera and Ojeda and the California Subclass Members regarding the unauthorized release and disclosure of the PII and PHI. Additionally, Defendant's conduct was "unfair" because it violated the legislatively declared policies reflected by California's strong data-breach, online-privacy, and medical-privacy laws, including the California Consumer Records Act, CAL. CIV. CODE §§ 1798.80, *et seq.*, the California CMIA, CAL. CIV. CODE §§ 56, *et seq.*, and the California constitutional right to privacy, CAL. CONST. ART. 1, § 1.

159. As a result of Defendant's unlawful and unfair conduct, Plaintiffs De Rivera and Ojeda and the California Subclass were damaged and injured by the significant costs of protecting themselves from identity theft and face ongoing and impending damages related to theft of their PII and PHI.

160. Defendant's wrongful practices constitute a continuing course of unfair competition within the meaning of the UCL because, on information and belief, Defendant has failed to adequately remedy its lax security practices or even fully

notify all affected California persons. Plaintiffs De Rivera and Ojeda and the California Subclass seek equitable relief pursuant to CAL. BUS. & PROF. CODE § 17203 to end Defendant's wrongful practices and require Defendant to maintain adequate and reasonable security measures to protect the PII and PHI of Plaintiffs De Rivera and Ojeda and the California Subclass.

161. Plaintiffs De Rivera and Ojeda and the California Subclass also seek an order requiring Defendant to make full restitution of all monies it received through its wrongful conduct, along with all other relief permitted under the UCL.

NINTH CLAIM FOR RELIEF
Injunctive/Declaratory Relief
(On Behalf of Plaintiffs and the Nationwide Class)

162. Plaintiffs incorporate by reference and reallege paragraphs 1-55 as if fully set forth herein.

163. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal and state statutes described herein.

164. Defendant owes a duty of care to Plaintiffs and Class Members, which required City of Hope to adequately monitor and safeguard Plaintiffs' and Class Members' PII and PHI.

165. Defendant and its officers, directors, affiliates, legal representatives, employees, co-conspirators, successors, subsidiaries, and assigns still possess the PII and PHI belonging to Plaintiffs and Class Members.

166. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' PII and PHI and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their PII and PHI. Plaintiffs

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

allege that Defendant's data security measures remain inadequate. Furthermore, Plaintiffs and the Class continue to suffer injury as a result of the compromise of their PII and PHI and the risk remains that further compromises of their private information will occur in the future.

167. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure the PII and PHI of Plaintiffs and the Class within its care, custody, and control under common law, HIPAA, and Section 5 of FTC Act;

b. Defendant breached its duty to Plaintiffs and the Class by allowing the Data Breach to occur;

c. Defendant's existing data monitoring measures do not comply with its obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect the PII and PHI of Plaintiffs and the Class within City of Hope's custody, care, and control; and

d. Defendant's ongoing breaches of said duties continue to cause harm to Plaintiffs and the Class.

168. This Court should also issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with legal and industry standards to protect the PII and PHI of Plaintiffs and the Class within its custody, care, and control, including the following:

a. Order Defendant to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Order that, to comply with Defendant's obligations and duties of care, City of Hope must implement and maintain reasonable security and monitoring measures, including, but not limited to:

i. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks,

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

penetration tests, and audits on Defendant's systems, networks, and servers on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

ii. Encrypting and anonymizing the existing PII and PHI within its servers, networks, and systems to the extent practicable, and purging all such information which is no longer reasonably necessary for Defendant to provide adequate healthcare services to its patients and other persons;

iii. Engaging third-party security auditors and internal personnel to run automated security monitoring;

iv. Auditing, testing, and training its security personnel regarding any new or modified procedures;

v. Segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems, networks, and servers;

vi. Conducting regular database scanning and security checks; and

vii. Routinely and continually conducting internal training and education to inform Defendant's internal security personnel how to identify and contain a data breach when it occurs and what to do in response to a breach.

169. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach or cybersecurity incident. This risk is real, immediate, and substantial. If another City of Hope data breach or cybersecurity incident occurs, Plaintiffs and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

170. The hardship to Plaintiffs and the Class if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Plaintiffs and the Class will likely be subjected to substantial, continued identity theft and other related

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

damages if an injunction is not issued. On the other hand, the cost of Defendant's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

171. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent City of Hope data breach or cybersecurity incident, thus preventing future injury to Plaintiffs and the Class and other persons whose PII and PHI would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Nationwide Class and California Subclass set forth herein, respectfully request that the Court order the following relief and enter judgment against City of Hope as follows:

A. Certifying this action as a class action under Federal Rule of Civil Procedure 23 and appointing Plaintiffs and their counsel to represent the Class and the California Subclass;

B. Declaring that City of Hope engaged in the illegal and wrongful conduct alleged herein;

C. Entering judgment for Plaintiffs, the Class, and the California Subclass;

D. Granting permanent and appropriate injunctive relief to prohibit Defendant from continuing to engage in the unlawful or wrongful acts, omissions, and practices described herein and directing Defendant to adequately safeguard the PII and PHI of Plaintiffs and the Nationwide Class and the California Subclass by implementing improved security controls;

E. Awarding compensatory, consequential, and general damages, including nominal damages as appropriate, as allowed by law in an amount to be determined at trial;

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220

F. Awarding statutory or punitive damages and penalties as allowed by law in an amount to be determined at trial;

G. Ordering disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendant as a result of Defendant's unlawful acts, omissions, and practices;

H. Awarding to Plaintiffs, Class Members, and California Subclass Members the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

I. Awarding pre- and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper; and

J. Granting such further and other relief as may be just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury for all claims and issues so triable.

Dated: April 30, 2024

By: */s/ Dustin L. Schubert*

Robert C. Schubert (S.B.N. 62684)
Amber L. Schubert (S.B.N. 278696)
Dustin L. Schubert (S.B.N. 254976)
SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
Telephone: (415) 788-4220
Fax: (415) 788-0161
rschubert@sjk.law
dschubert@sjk.law
aschubert@sjk.law

Counsel for Plaintiffs Joseph De Rivera, Irwin Ojeda, and d'Amileau Baulk and the Putative Classes

SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, CA 94123
(415) 788-4220